[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G07F 7/10 (2006.01)
G06K 19/07 (2006.01)

[12] 发明专利说明书

专利号 ZL 200580019417.1

[45] 授权公告日 2009 年 6 月 17 日

[11] 授权公告号 CN 100501779C

[22] 申请日 2005.4.13
[21] 申请号 200580019417.1
[30] 优先权
[32] 2004.4.13 [33] DE [31] 102004018367.8
[86] 国际申请 PCT/DE2005/000648 2005.4.13
[87] 国际公布 WO2005/101333 德 2005.10.27
[85] 进入国家阶段日期 2006.12.13
[73] 专利权人 SAP 股份公司
地址 德国瓦尔多夫
[72] 发明人 奥利弗·伯索尔德
[56] 参考文献
WO0143065A1 2001.6.14
US2004066278A1 2004.4.8
US2004054900A1 2004.3.18
CN1349639A 2002.5.15
US5640002A 1997.6.17
US6104281A 2000.8.15
审查员 罗 强
[74] 专利代理机构 北京市柳沈律师事务所
代理人 邵亚丽 李晓舒

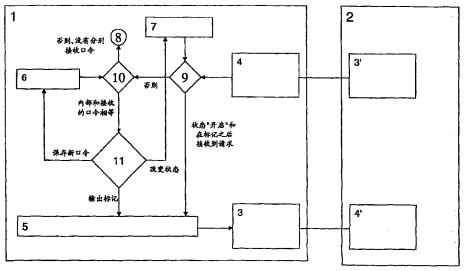
权利要求书 4 页 说明书 10 页 附图 3 页

[54] 发明名称

利用所有者控制的射频标识标签功能的数据保护射频标识系统

[57] 摘要

本发明涉及一种 RFID 标签，具有 a)用于由读取器(2)生成的数据的发射设备(4)和接收设备(3)；b)特别是用于标识数据的存储器(5)，清楚地标识 RFID 标签；c)控制单元，根据读取器(2)的下列事实自动执行功能：检测内部口令存储器(6)中的内部口令的知识、和/或基于存储在内部状态存储器(7)中的信息允许该功能的执行；和 d)用于改变，特别是根据内部口令与由读取器(2)接收的口令的在先比较来改变，存储在存储器中的内部口令和/或内部状态的改变单元。 本发明还涉及使用该 RFID 标签的方法。 本方面解决了 RFID 技术的私密问题，并且使得与已知的停用功能不同，还可以进一步使用所述技术，以用于具有本发明的 RFID 标签的、有选择地网络连接的智能设备。



1. 一种 RFID 标签，具有

a）用于来自读取器（2）的数据的发射设备（4）和接收设备（3），

b）控制装置，根据读取器（2）的下列事实自动执行功能：

- 证明用于内部口令的存储器（6）中的内部口令的知识，和/或

- 存储在用于内部状态的存储器（7）中的信息允许所述功能的执行，和

c）用于改变，特别是根据内部口令与从读取器（2）接收的口令的在先比较，来改变所存储的口令和/或内部状态的装置，

d）用于 RFID 的无歧义的标识数据的存储器（5），

e）用于存储验证值的不可重写或可重写存储器，和

f）用于由两个输入值确定测试值的装置，其中由使用接收的值和验证值作为该装置的输入、并且可以发送结果的事实，来提供验证标识数据的功能。

2. 如权利要求 1 所述的 RFID 标签，具有用于存储内部口令的可重写的存储器（6）。

3. 如权利要求 1 或 2 所述的 RFID 标签，具有用于比较两个值的第一比较装置（10），其中可以用该第一比较装置（10）比较接收的值与存储的口令。

4. 如权利要求 1 所述的 RFID 标签，其特征在于，具有用于生成随机值的随机化装置（12）。

5. 如权利要求 1 所述的 RFID 标签，其特征在于，具有用于由至少两个输入值计算一个或多个测试值的测试值装置（14）。

6. 如权利要求 1 所述的 RFID 标签，其特征在于，具有用于比较所存储的口令或者用于验证标识数据的询问-应答功能。

7. 如权利要求 3 所述的 RFID 标签，具有用于缓存随机值的瞬时或非瞬时、可重写的缓冲器（13）。

8. 如权利要求 7 所述的 RFID 标签，其中，可以回答来自读取器（2）的、用于比较所存储的口令与缓冲器以及发送用随机化装置（12）生成的随机值的质询。

9. 如权利要求 8 所述的 RFID 标签，其中，第一比较装置（10）将对发送的回答与测试值装置（14）的结果进行比较，其中使用来自缓冲器的随机值与来自存储器（6）的内部口令作为第一比较装置（10）的输入，或者使用

对读取器发送的随机值的回答以及测试值装置的结果作为第一比较装置（10）的输入。

10. 如权利要求 3 所述的 RFID 标签，其中，通过第一比较装置（10）的正的比较结果，内部口令验证被评估为成功，否则评估为不成功。

11. 如权利要求 1 所述的 RFID 标签，具有用于至少部分标识数据的传输的装置和/或用于内部状态的存储器（7），其中内部状态定义是否允许输出标识数据以及允许输出哪部分标识数据。

12. 如权利要求 11 所述的 RFID 标签，其中，部分标识数据的传输的功能由第二比较装置（9）根据内部状态实现。

13. 如权利要求 10 或 11 所述的 RFID 标签，其中，仅当在先的口令验证成功时，才可以执行标识数据的传输，其中在成功的情况下，可以完整地传输标识数据。

14. 如权利要求 10 或 11 所述的 RFID 标签，其中提供仅在成功的口令验证之后才执行的改变内部状态的功能。

15. 如权利要求 1 所述的 RFID 标签，具有用于由两个输入值计算新口令的装置，两个输入值是接收值以及来自用于密码的存储器的值。

16. 如权利要求 15 所述的 RFID 标签，其中，提供改变口令的可能性，其中所计算的新口令被存储在用于内部口令的存储器（6）中，并且仅当在先的口令验证成功时，才执行改变口令的功能。

17. 如权利要求 1 所述的 RFID 标签，其中，直接接收新口令并且该直接接收的新口令存储被存储在用于内部口令的存储器（6）中，并且提供改变口令的可能性，仅当在先的口令验证成功时，才执行改变口令的功能。

18. 如权利要求 1 所述的 RFID 标签，其特征在于这样的事实，可以与制造商合作验证从 RFID 标签发送的标识数据的真实性。

19. 如权利要求 1 所述的 RFID 标签，具有特殊的属性，即，仅对根据权利要求 12 的特定状态执行各项功能，或者仅在根据权利要求 10 的口令验证之后执行各项功能。

20. 如权利要求 1 所述的 RFID 标签，具有特殊的属性，即，提供额外存储器，该额外存储器仅可以针对权利要求 12 所述的特定状态被访问，或者仅可以在根据权利要求 10 的口令验证之后被访问。

21. 一种读取器，具有用于与根据权利要求 1 的 RFID 标签通信的装置，

所述读取器:

a）具有用于证明存储在根据权利要求 2 的 RFID 标签中的口令的装置，

b）用于存储的数据的质询装置，

c）用于改变 RFID 标签的内部状态和 RFID 标签的口令的装置。

22. 如权利要求 21 所述的读取器，具有用于读取器口令的存储器（6’）和/或用于计算测试值的装置，其中该装置实现与根据权利要求 5 的测试值装置（14）相同或相反的计算。

23. 如权利要求 22 所述的读取器，具有用于发送读取器口令的装置。

24. 如权利要求 22 所述的读取器，具有下列功能的一个或多个:

使用接收的随机值和读取器口令作为所述读取器的测试值装置（14’）的输入，并且将结果发送到 RFID 标签的功能，

用于在口令验证之后、质询 RFID 标签的标识数据的功能，

用于在口令验证之后、改变根据权利要求 11 的 RFID 标签上的内部状态的功能，

用于在在先口令验证之后、改变根据权利要求 4 的 RFID 标签上的内部口令的功能，其中以明文传输新口令，或者在装置的帮助下由在先的和新的口令计算测试值，并且将该测试值发送到 RFID 标签。

25. 一种用于如权利要求 21 所述的读取器的处理方法，用于验证根据权利要求 1 的 RFID 标签的标识数据，其中

a）读取器将随机值发送到 RFID 标签，并且将接收的测试值、随机值和标识数据发送到带有 RFID 标签的产品的制造商，以及

b）如果验证成功，则制造商用“真”回答。

26. 如权利要求 25 所述的处理方法，其中，读取器（2）事先要求制造商对于标识数据的随机值和测试值的有效组合，并且将 RFID 标签的回答与在组合中含有的测试值进行比较。

27. 如权利要求 25 或 26 所述的处理方法，其中，使用数据库来存储对于所有制造的产品的标识数据，并且使用该数据库来存储验证值。

28. 如权利要求 27 所述的处理方法，所述数据库具有这样的功能：为了正确性而测试对标识号、随机值和由 RFID 标签所计算的回答的质询，以及使用由接收的随机值和验证数据计算测试值的装置而向质询部件提交测试的结果。

29. 如权利要求28所述的处理方法，其中，在用于生成随机值的装置和权利要求28的计算测试值的装置的帮助下，准备标识数据、随机值和测试值的组合。

30. 一种用于改变存储在如权利要求1所述的RFID标签上的口令的处理方法，其特征在于这样的事实，

a）读取器（2）首先证明根据权利要求23或24的在先口令的知识，以及

b）然后提交根据权利要求24的新口令。

31. 如权利要求30所述的处理方法，用于将根据权利要求1的读取器在一段时间中接触的所有RFID标签的口令改变为共同口令，该共同口令要么是预定义的，要么是在所述处理方法的开始时随机选择的，并且可以控制该共同口令。

32. 如权利要求30所述的处理方法，用于改变根据权利要求1所述的RFID标签的所有者，其中每个RFID标签执行两次根据权利要求30的口令改变，其中使用随机选择的中间口令。

利用所有者控制的射频标识标签功能的数据保护射频标识系统

技术领域

本发明涉及如权利要求 1 前序部分所述的 RFID 标签。

本申请涉及所谓的 RFID（射频标识）系统的功能的增强。

背景技术

RFID 标签和必要的基础设施（例如，读取器）在现有技术中已经公知了很长时间，并且例如，用于标记物品。RFID 标签通常包括发射和接收设备，利用这些发射和接收设备，一旦 RFID 标签处于其有效范围内，RFID 标签除执行其它功能外，还可以将标记（标识数据）发送到读取器，并且可以执行由读取器命令（调用）的其他功能。

标记用于标识 RFID 标签以及与其相关的物品。在不久的将来，这些 RFID 标签可以取代在先在消费品上使用的条形码，以便简化后勤处理以及超市中的处理。

例如，由于具有 RFID 标签的购物车的物品可以在一个步骤中完全扫描，因此部署自助收银机。

本发明要解决这种技术的私密问题：由于每个 RFID 标签应当带有唯一的序列号，因此，甚至在离开超市之后，每个消费品—这里是指每个个人物品—的路径可以在未经注意的情况下被读出。因此，人们可能在这些序列号的帮助下被跟踪，并且还可能被任何人扫描关于他们随身携带的所有产品（例如，他们的衣服）。如果这些数据在数据库的帮助下被收集、存储并且评估（这至少是值得担心的），那么数据保护人员和私密积极分子所担心的“玻璃人”的情景将变成现实。

以前，行业内仅仅用所谓的停用（kill）功能来对付这种情形，例如在付款后，用该功能可以使 RFID 标签永久地失效。不幸的是，RFID 的永久失效妨碍了许多应用。特别是，通常在产品购买后才开始使用的应用受到影响，例如，一种智能洗衣机，它在放入其中的衣物的件数的帮助下自动确定洗涤

温度和程序。在 EPGglobal 的规范版本 1.0 中描述了可使用这样的停用功能的 RFID 标签（http://epcglobalinc.org/standardstechnologie/specifications.html）。

发明内容

本发明在网络连接具有根据权利要求 1 特征的 RFID 标签的设备、根据权利要求 29 特征的读取器、和根据权利要求 42 特征的处理的给定情况下，解决了先前的 RFID 技术的所述私密问题，并且同时，与已知的停用功能不同，还使得智能技术的使用成为可能。

由每个从属权利要求得出有利的进一步的实施方式。下面，重复地参考通过 RFID 标签区别产品的示例。该示例仅仅是根据本发明教学的典型应用。本领域技术人员将认识到也可以构思出其他用途。

本发明通过 RFID 标签的（标识）功能的动态激活、失效或限制的可能，增强了 RFID 标签的功能。具体地说，意思是，在内部状态的帮助下，在接收到来自读取器的特定请求时决定 RFID 执行哪些功能以及执行到什么程度。具体地说，提供一种其中 RFID 标签不输出任何内部存储的数据的状态，这通常使得标识成为可能。

然而，在每个状态中，RFID 标签应当满足读取器与 RFID 标签之间的通信协议到这样的程度，即，数据和命令的发送和接收是可能的。

例如，RFID 标签必须通过读取器通知其存在，并且加入所谓的单数（singulation）或反共谋协议，以便能够完全接收单独的命令。在上述 EPCglobal 规范中，提出了反共谋协议，其不使用存储的标识数据运行。

在 DE 101 61 302 中，提出了基于有规律再生的随机值、而非标识数据的反共谋协议。

RFID 标签的有利实施方式提供改变内部状态的功能。这里，该功能仅在调用功能的读取器证明(demonstrate)具有秘密(secret)数据集的知识、存储在 RFID 标签中的位序列之后才被执行。秘密数据集在下面指代为口令。检测功能在下面指代为验证。

RFID 标签的其他实施方式提供用于存储口令的可重写、非瞬时存储器。其中，在 RFID 标签的生产过程期间或者在产品到 RFID 标签的连接期间，可以以有利的方式设置第一口令。理想地，口令的写入应当与标识数据的写入同时发生，因为它们两个都在产品后勤链(logistics chain)的每个步骤中发送。

根据本发明的RFID系统中披露了口令验证的两个有利实施方式:

在第一实施方式中，从读取器向 RFID 标签发送口令。该验证方法的优点是 RFID 标签非常简单的可实现性。只需要一个比较存储的口令与接收的口令的功能。缺点是其他设备可以通过窃听无线通信来确定口令。

在第二实施方式中，RFID标签以及读取器中可以有一个装置（这里也称为“功能”），它组合口令与另一值来形成一个测试值。此外，在 RFID 标签中可以有用于生成随机值的随机化装置。用于生成随机值的随机化装置的实施方式（即，算法的选择）原则上是任意的。例如，可以使用采样电路（例如二极管）的噪声源，或者可以将 hash(散列)函数重复地应用到在生产期间单独产生的初始值，并且可以从各个中间值的部分形成随机序列。用于计算测试值的装置可以任意地实现。密码安全单向函数或者对称加密函数将是理想的，其中使用输入值之一作为密钥，因为这样逆反函数或者由另两个值的知识确定未知的第三值将是困难或不可能的。

实现测试值装置的选择还包括仅基于输入值执行计算的可能，其中仅使用内部口令或使用另外的任意装置来将组合输入值。实现测试值装置的选择还包括基于多于两个的输入值执行计算的可能。实现测试值装置的选择还包括计算多于一个输出值的可能。

在验证的这个实施方式中， RFID 标签首先生成随机值，将其存储在存储器中，并且将随机值另外发送到读取器。读取器使用测试值装置，其中使用口令和接收的随机值作为输入。读取器将测试值发送到 RFID 标签。RFID 标签在所存储的口令与所存储的随机值的帮助下计算第二测试值，并且比较这两个测试值。如果两个测试值一致，则执行受验证保护的功能。

或者，RFID标签上的装置也可以反向计算，即，由测试值和输入值计算当前另一输入值，并且比较它们。验证的第二实施方式的优点是防止窃听的安全性。缺点是RFID标签的电路技术的复杂度更高。

处理的安全性、进而保护口令不被第三方确定的能力取决于测试值装置的加密质量（即，逆反单向函数或确定未知值有多难）、随机值生成器的加密质量、以及用于口令、随机值和测试值的位序列的长度。

此外，根据本发明的 RFID 标签的一个实施方式提供用于改变口令的装置（功能）。这里，仅在成功验证在先口令之后才执行该功能。这里，新的口令从读取器发送到RFID标签。

披露了从读取器将口令发送到RFID系统的两个有利的实施方式:

在口令发送的第一实施方式中，新口令从读取器发送到 RFID 标签。本发明的该实施方式的优点是 RFID 标签上的简单的可实现性。缺点是可能被另一设备窃听。

在口令发送的第二有利实施方式中，在 RFID 标签和读取器中提供可以由两个输入值计算第三值的装置。该装置可以以任意方式实现，其中该计算必须可逆到存在可以由输入值之一和输出值计算第二输入值的装置的程度。该装置的一个示例是任意的对称加密函数或者两个输入值的逐位 XOR 叠加。用于实现该装置的选择还包括基于多于两个的输入值执行计算的可能。实现该装置的选择还包括计算多于一个的输出值的可能。

本发明的该实施方式的优点是更强的防窃听的安全性。缺点是 RFID 标签的电路技术的复杂度更高。处理的安全性取决于使用的装置的加密质量，以及使用的值的长度，其中简单的逐位 XOR 叠加（一次性垫，one-time pad）已经提供了最大安全性，因此是最优的。

这样可以改变 RFID 标签的口令或状态，因此需要 RFID 标签的当前所有者知道当前口令。

与基于停用功能（EPC 标准）的在先实施方式相反，在本发明的情况下，在收银机处时或之后将口令送给消费者（例如，通过在收据上打印出来）。因此，消费者对她/他的 RFID 标签的功能获得完全控制。

通过改变口令，当前所有者接管 RFID 标签功能的单独控制，由于在先的所有者在其数据库中存储了不正确的口令。

本发明还涉及一种用于改变口令的有益处理，它解决了不能够标识处于失效状态的 RFID、从而无法确定谁的口令的问题。

该有益处理包括：所有者将同一口令存在她/他所拥有的所有 RFID 标签中。仅当这样做时或者在这之后才失效。理想地，该处理应当已经例如在超市收银机中执行。

例如在超市收银机处改变 RFID 标签的所有者，应当以两步进行:

1. 先前所有者将 RFID 标签的口令改变为随机选择的值。在交易物品时，旧所有者将使用的口令传递给新所有者。

2. 新所有者尽可能在无线范围之外（在她/他的机密区域中）执行口令的第二次改变，其中所有者通常使用对所有她/他的 RFID 标签共同（common）

的口令。

在超市收银机处的有益步骤序列是:

1. 读取器选择随机值作为新口令。

2. 读出 RFID 标签的标识。

3. 将 RFID 标签的口令改变为新的值，读取器通过质询数据库（例如，超市的产品库存数据库）接收当前所需的先前口令。

4. 使 RFID 标签无效。

5. 如果存在其他的 RFID 标签，继续步骤 2。

6. 将这次购物的口令提交给产品的新所有者，例如，通过在收银机收据上打印，或者通过发送给消费者所拥有的设备（例如芯片卡）。

这样，个人或家庭拥有的所有 RFID 标签具有相同的口令，口令的改变应当在此人的机密区域中由读取器重复。

在这样做时，可以使用类似的步骤序列，区别在于，只执行一次步骤 1，并且对所有 RFID 标签使用一次存储在设备中的口令。在步骤 3 中必需的在先口令可以通过口令的先前改变的步骤 6 由用户得到，并且在给定情况下必须发送到读取器。省略步骤 6。

对于如何将中间口令传递给用户，提出了三种可能。

1. 发送给消费者拥有的任何电子设备（例如，蜂窝电话）。

2. 直接发送到消费者的室内系统（尤其是通过因特网远距离销售/订购）。

3. 打印在收银机收据上：在该技术的起始阶段中，如果只有很少消费者具有智能家庭设备，则第三种可能尤其重要。当获得这样的设备时，一个人可以（可以说是）反向地迁入重要的 RFID 标签。另一方面，通过这种方式，可以在没有存储口令的电子设备的情况下购买。

在本发明的另一有利实施方式中，所有者的改变仅仅通过传送先前口令来完成。这种可能是在特定环境下，实践中在超市收银机上，因为 RFID 标签在生产期间被分配了单独的口令。然而，并不推荐该处理来进行从一个机密区域到另一机密区域的传输，因为在这种情况下，对先前所有者的所有 RFID 标签共同的口令将不得不被传递给新所有者。

本发明解决了涉及离开超市后的所有处理的、RFID 技术的所述私密问题，因为失效的 RFID 标签仅对授权的扫描仪标识自己。

由于基于口令限制对 RFID 标签功能的访问的可能性，因此 RFID 标签智

能被验证的读取器完全控制。通过改变口令，可以将 RFID 标签的控制限制到当前用户。此外，所有者可以任意地限制未授权方的访问。将可以构思出下列示例性限制：

- 完全匿名化（anonymization）：未验证的读取器接收不到标记的任何部分，即，RFID 标签不可标识。
- 序列号匿名化：可以使用 RFID 标签，从而它们输出 EPC（电子产品代码），包括产品代码和各个物品的序列号。在该实施方式中只输出产品代码。产品的具体物品内容目前仍被隐藏。
- 标识号匿名化，但披露其他信息：标识号的输出限制于经验证的读取器，但本发明的进一步的实施方式中通过经验证的读取器可以改变的、可通过其他功能调用的任意其他信息，通常是可得到的。这使得例如以如下方式构建关于化学成分的循环信息成为可能，即，它可读、或者用于在自动返回设备中关于存放所需的包装信息。

本发明另一有利实施方式提供一种由两个输入值计算测试值的装置。该装置的实现示例是加密 hash 函数（单向函数）或对称加密函数。在询问-应答（challenge-response）处理的帮助以及与 RFID 标签或产品制造商的合作下，可以检查 RFID 标签的真实性、以及也带有约束检查产品的真实性。

本发明的进一步的实施方式的背景是这样的事实，即，可以没有问题地生产自由编程的 RFID 标签，由于生产技术，几乎所有 RFID 标签被允许在没有具体的标识号的情况下生产，而它们只接收它们对产品最初和最后的编程。没有可验证的标识号的 RFID 标签将使得产品的错误（corruption）更容易，而不是更难。

对于该实施方式，在根据本发明的 RFID 标签中，必须与口令一同存储额外的秘密值，它可以存储在不可重写的存储器中。此外，在产品或 RFID 标签制造商的计算机系统中，必须提供可以重复或逆反 RFID 标签中的装置的计算的装置。此外，读取器通常需要在线连接到制造商的计算机系统。制造商还需要数据库，对每个 RFID 标签存储至少标识号和存储在 RFID 标签中的秘密值。

在要求保护的处理的实施方式中，读取器向 RFID 标签发送随机值。RFID 标签在装置的帮助下计算测试值，其中使用存储在 RFID 标签中的秘密值和随机值作为输入。测试值被发送回到读取器。读取器将 RFID 标签标识数据、

随机值和测试值的组合发送到制造商。制造商在其装置和存储在其数据库中的所质询的 RFID 标签的秘密值的帮助下，测试正确性。在这样做时，根据该装置的实施方式，使用三个值（RFID 标签的随机值、测试值和秘密值）中的两个作为输入值，并且将结果与第三值比较。制造商将比较结果报告给读取器。

在处理的另一有利的实施方式中，读取器已经事先接收了特定 RFID 标签的随机值和测试值的一个或多个有效组合。然后通过将组合中包含的随机值送到 RFID 标签，并且将 RFID 标签的应答与测试值比较，可以本地进行 RFID 标签的真实性测试，而不必有在线连接。

应用的组件另外是（网络连接的）、具有下列特定功能的读取器:

- 验证功能（发送口令或询问-应答处理的执行和用于检测口令的知识的相应装置）
- 在口令验证之后调用功能
- 用于改变状态的功能
- 用于改变口令的功能
- 用于存储共同口令并且仅转发给其他已知可信的设备的方法
- 通过将口令改变为共同口令指定当前口令、拥有新 RFID 标签的方法。

本发明实施例不限于上面指定的优选实施例。相反，可以构思出许多利用根据本发明的教导的变型（甚至具有根本不同类型的实施例）。

附图说明

下面参照若干实施例中的附图详细描述本发明。其中:

图 1 是根据本发明第一实施方式的、与读取器合作的 RFID 标签的数据流程的示意图，

图 2 是根据本发明第二实施方式的、具有安全口令验证的 RFID 标签的数据流程的示意图，

图 3 是根据本发明的处理标签的流程图。

具体实施例方式

在图 1 中示出第一实施方式，其中示出根据本发明的 RFID 标签的简单实施方式。

RFID 标签 1 包括存储器 5，该存储器 5 含有该标签自身的、无歧义（unambiguous）的标记。通过该标记，它可以与其他标签无歧义地区分开来。

此外，RFID 标签 1 包括用于内部口令的存储器 6。

此外，RFID 标签 1 包括用于内部状态的存储器 7，该内部状态指定是否可以执行特定功能。

在工作期间，在 RFID 标签 1 与读取器 2 交互。RFID 标签 1 或读取器（2）每一个包括用于可以与标准完全不同的数据的发射设备 3、3'和接收设备 4、4'。

在图 3 中分别说明各个质询，以便对其参考。

首先，从读取器 2 到 RFID 标签进行标签的质询。可替代地或者另外地，可以指定口令。

在图 1 的第二比较装置 9 中，检查 RFID 标签 1 的内部状态。它要么是“开启(open)”，要么是“封锁(blocked)”，并且作为标志存储在存储器 7 中。

如果 RFID 标签是“封锁”，则存储器 5 的无歧义的标记只输出到证明具有存储器 6 中存储的内部口令的知识的授权读取器 2。

在图 1 的第一比较装置 10 中，将内部口令与在给定情况下从读取器读入的口令（读取器口令 6'）进行比较。

如果没有从读取器 2 读入口令，或者口令不一致，则处理以最终状态 8 终止。可选地，可以输出出错消息。

如果内部口令与接收的口令一致，则执行读取器 2 所请求的功能。通过分支设备 11，确定：

- 从存储器 5 输出无歧义的标记，
- 改变存储器 7 中的内部状态，
- 将新的内部口令存储在存储器 6 中。

这样做时，很重要的是，存储在 RFID 标签 1 中的每个值（其作用是无歧义地标识物品，因而对每个物品是不同的）表示 RFID 标签 1 的无歧义的标记 5。

在替代实施方式中，根据权利要求 9 到 11 的比较序列可以按任意次序执行。此外，在所有质询中（除了在标记之后）对状态的检查可以被省略。

此外，作为另一选择，可以在最终状态 8 中向读取器 2 发送出错消息等。原则上，是否和如何将状态或口令改变发送回读取器 2 是任意的。

此外，应当保护改变口令和封锁状态的组合（作为函数调用）。

图 2 示出具有图 1 中表示的所有功能的 RFID 标签 1，从而可以参考上述描述。然而，口令验证是以特别安全的方式进行的。这通过两个步骤进行:

a）首先调用功能，

b）然后（如果 RFID 标签 1 是封锁的）发送随机值，读取器利用该值发送加密的口令—如果成功，则执行在先请求的功能。下面对此详细描述。

在图 1 中所述的实施方式的修改形式中，这里在第二比较装置 9 中进行变更的处理。如果内部状态（见存储器 7）是封锁的，则使用随机值生成器 12 生成随机值。随机值被存储在缓冲器 13 中。

随后，将该随机值通过发射设备 3 送到读取器 2。

由测试值装置 14 将该随机值与来自存储器 6 的内部口令一起并行处理。测试值装置 14 由这些数据计算唯一的测试值。

读取器 2 原则上具有同样的信息，即，读取器口令 6'和接收的随机值。使用可比较结构的测试值装置 14'，在读取器 2 中也确定测试值，并且将其发送到 RFID 标签 1。

在第一比较装置 10 中，执行 RFID 标签 1 所生成的测试值与读取器 2 所生成的测试值之间的比较。

如果测试值一致，则使用分支设备 11 进行图 1 所示的进一步处理。

如果测试值不一致，则类似于图 1 执行终止。

此外，在存储器 6 中提供用于改变内部口令的装置 15。该装置 15 由在先的内部口令和读取器 2 接收的值，生成新的内部口令。分支设备 11 在这种情况下输出相应命令。

于是，如果需要的话，RFID 标签 1 质询口令。该处理是权利要求 5 到 11 的内容。

图 3 示出根据图 1 或 2 的处理的一个实施方式的顺序。其中描述了无歧义的标记的质询和随后口令的改变（以便由所有者接受）和后面的 RFID 标签的内部状态的框。

使用该处理，电子所有者接受是可能的。标签的内部口令的知识具有与“所有者”的状态相同的含义。

附图标记列表

1 RFID 标签

2 读取器

3 RFID 标签的发射设备

4 RFID 标签的接收设备

3' 读取器的发射设备

4' 读取器的接收设备

5 用于 RFID 标签的无歧义标记的存储器

6 用于内部口令的存储器

6' 用于读取器口令的存储器

7 用于内部状态的存储器

8 最终状态，可选地输出出错消息

9 第二比较装置、状态、接收的质询

10 用于接收和存储的值的第一比较装置

11 根据从读取器接收的质询的分支设备

12 随机值生成器（随机化装置）

13 用于随机值的缓冲器

14 RFID 标签的测试值装置、计算函数（由一个或多个输入值计算输出值，其中不能由输出值重构出输入值，例如，hash 函数）

14' 读取器的测试值装置

15 用于计算新口令的装置

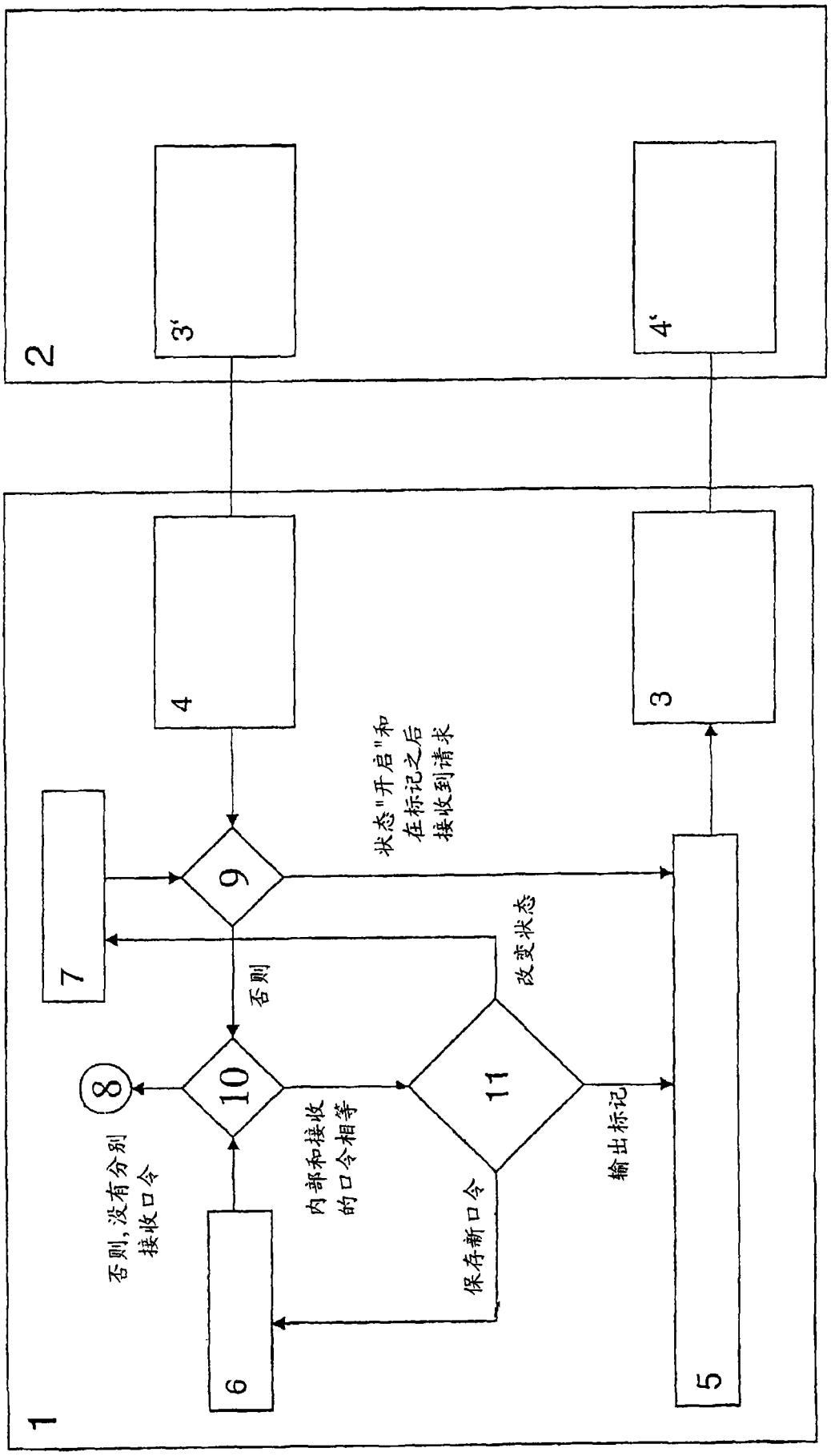
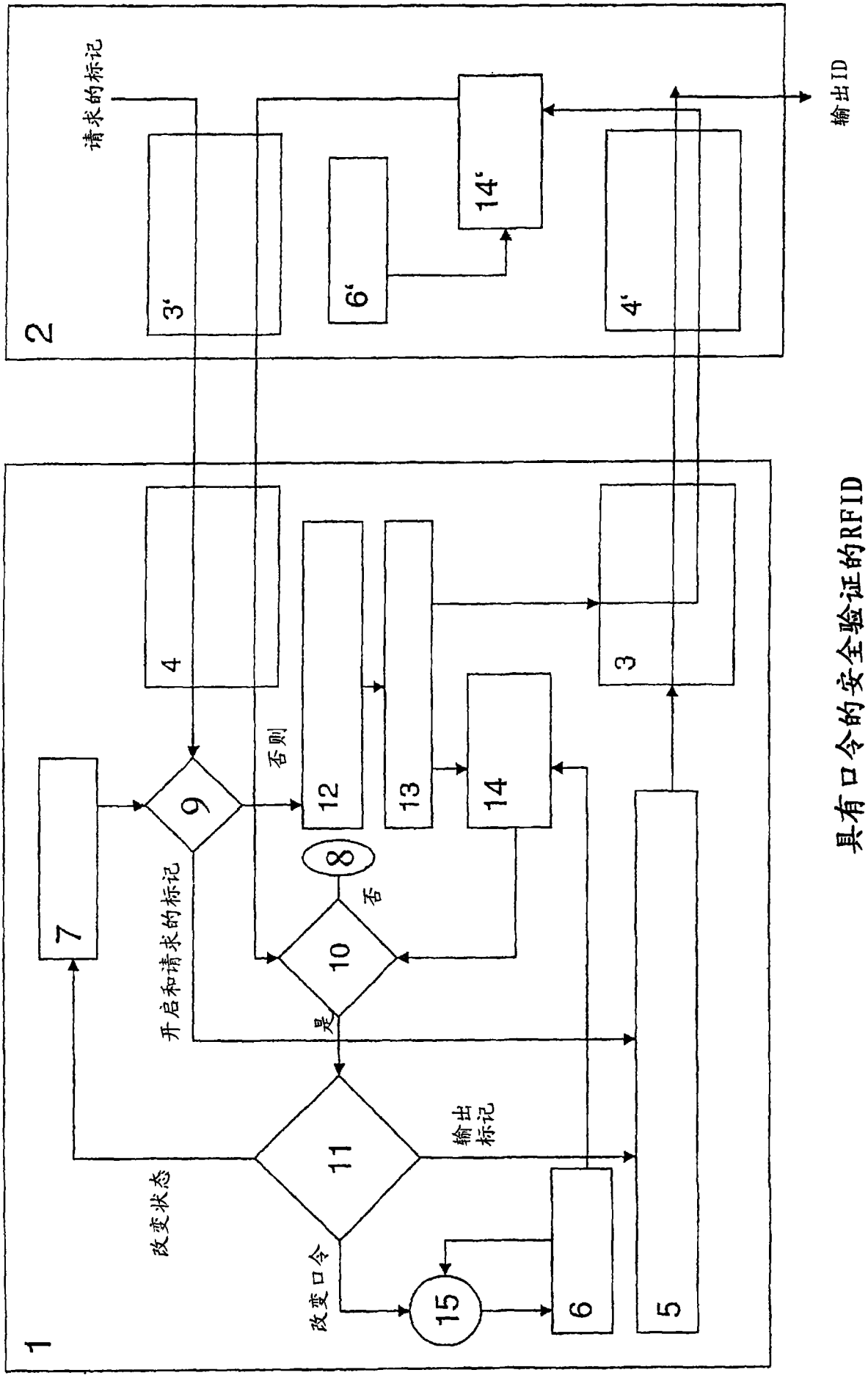

1
2
3
3'
4
4'
5
6
7
8
9
10
11
状态"开启"和
在标记之后
接收到请求
否则
改变状态
否则,没有分别
接收口令
内部和接收
的口令相等
保存新口令
输出标记

图 1



具有口令的安全验证的RFID

图 2

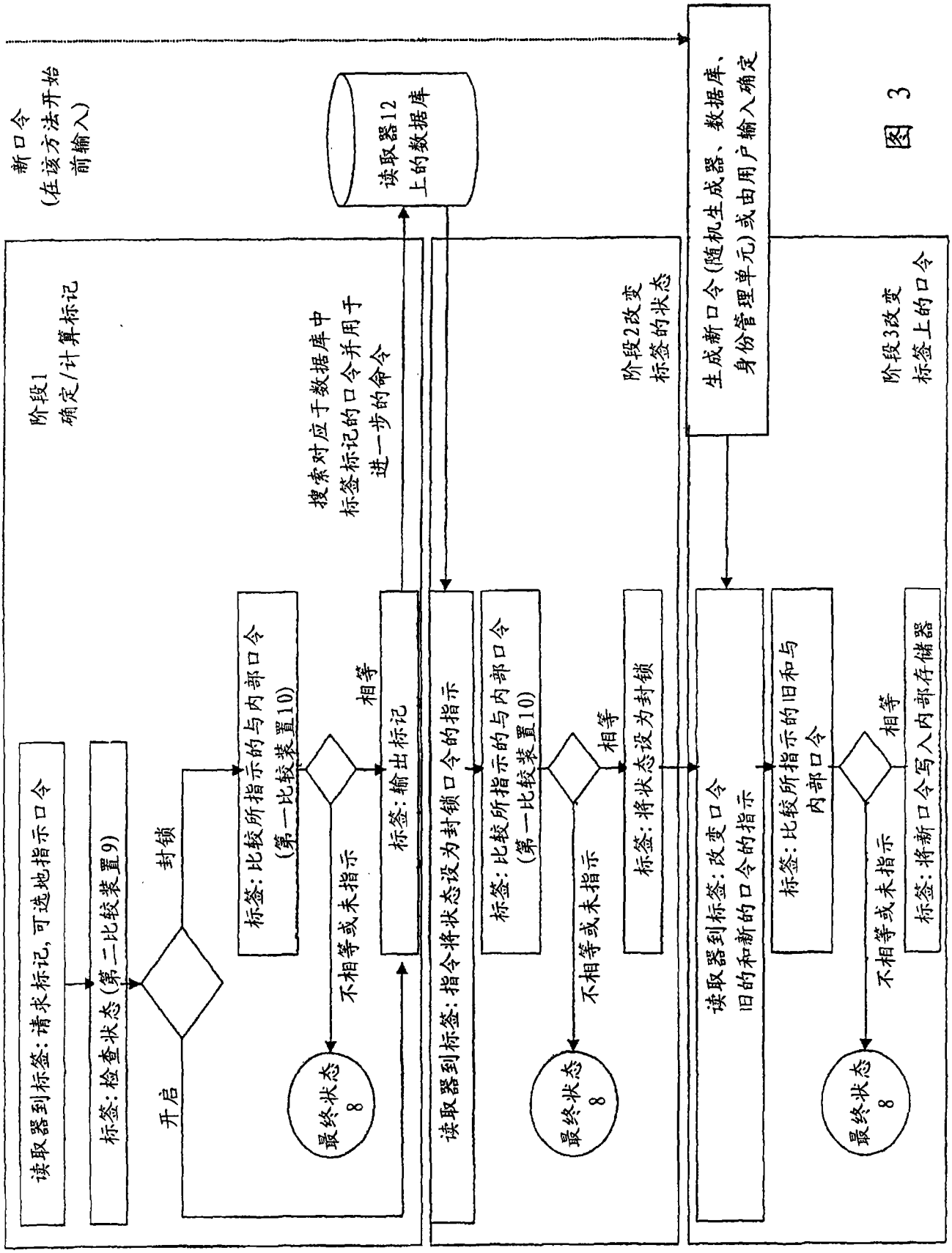

新口令
(在该方法开始前输入)
读取器12上的数据库
阶段1
确定/计算标记
读取器到标签:请求标记,可选地指示口令
标签:检查状态(第二比较装置9)
封锁
开启
标签:比较所指示的与内部口令(第一比较装置10)
不相等或未指示
最终状态8
相等
标签:输出标记
搜索对应于数据库中标签标记的口令并用于进一步的命令
读取器到标签:指令将状态设为封锁口令的指示
标签:比较所指示的与内部口令(第一比较装置10)
不相等或未指示
最终状态8
相等
标签:将状态设为封锁
阶段2改变标签的状态
生成新口令(随机生成器、数据库、身份管理单元)或由用户输入确定
读取器到标签:改变口令旧的和新的口令的指示
标签:比较所指示的旧和与内部口令
不相等或未指示
最终状态8
相等
标签:将新口令写入内部存储器
阶段3改变标签上的口令

图 3